JW

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,218	11/26/2001	Pasi Into Loukas		8034

7590 04/07/2005

Pasi Loukas
Kemintie 969
Rovaniemi, 96700
FINLAND

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 04/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)	
	09/993,218	LOUKAS, PASI INTO	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are examined.

Claim Objections

2. Claims 2, 5, 6, 13, 18, 19 are objected to because of the following informalities: the claims language discloses "a said" phrase. Appropriate correction is required.

3. Claim 23 is objected to because of the following informalities: "it is not done said identification comparison, and said identification of said file is not delivered to an anti-virus host computer" may have grammatical error. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 5-9, 12, 16, and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claims 5-9, 12, 16, and 27 recites the limitation "(a) through (c)" or "(a) and/or (b)" in claim language. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-4, 10, 14, 15, 20, and 23 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Hypponen et al. U.S. Pub. No. 20030191957 (hereinafter Hypponen).

9. As per claim 1, Hypponen discloses a network based anti-virus system especially for wide area networks, like the Internet, comprising: client computer(s), which are any computers in the network (Hypponen: [0006]-[0010]); anti-virus host computer(s), which are any computers in the network chosen for that purpose (Hypponen: [0006]-[0010]; [0032]); wherein identification(s) of file(s) or other web content is delivered from a client computer to an anti-virus host computer (Hypponen: [0006]-[0010]; [0035]); wherein said anti-virus host computer compares each of said delivered identification(s) to stored identifications of files or other web content, and on the basis of the results of said comparison either: (a) it is performed safety measures, (b) and/or, said client computer and/or the user of said client computer is informed about the results of said comparison, (c) or, no specific actions are performed (Hypponen: [0006]-[0010] and [0035] and [0038]: intercept the data and identify if the data is of a type capable of containing a virus).

10. As per claim 2, Hypponen discloses a network based anti-virus system according to claim 1, Hypponen further discloses the system comprising: wherein a said stored identification either: (a) belongs to a specific file or other web content, (b) does not belong to any specific file or other

web content, but is rather an identification filter, (c) or, partly belongs to a specific file or other web content, and partly is a identification filter (Hypponen: [0035]).

11. As per claim 3, Hypponen discloses a network based anti-virus system according to claim 2. Hypponen further discloses the system comprising: wherein said delivered identification(s) is delivered when said client computer downloads from the network said file(s) or other web content to which said delivered identification(s) belong (Hypponen: [0006]-[0010]; [0035]: intercept the data and check).

12. As per claim 4, Hypponen discloses a network based anti-virus system according to claim 3. Hypponen further discloses comprising: wherein said delivered identification(s) is delivered to said anti-virus host computer either: (a) before said downloading, (b) during said downloading, (c) or, after said downloading (Hypponen: [0006]-[0010]).

13. As per claim 10, Hypponen discloses a network based anti-virus system according to claim 4. Hypponen further discloses the method comprising: wherein said anti-virus host computer does not specifically fight against viruses; wherein the purpose of said comparison is to find out if said inspected files and other web content are or are not non-wanted/unacceptable instead of if they are possibly virus infected (Hypponen: [0006]-[0010]; [0035]-[0038]).

14. As per claim 14, Hypponen discloses a network based anti-virus system according to claim 3. Hypponen further discloses the system comprising: intermediate computer(s), which are

able to prevent downloading of files and / or other web content from the network to a client computer (Hypponen: [0006]-[0010]; [0038]).

15. As per claim 15, Hypponen discloses a network based anti-virus system according to claim 14. Hypponen further discloses the system comprising: wherein a said intermediate computer is: (a) a server of the local area network, (b) a server of the internet service provider, (c) a network node computer, (d) or, a source host computer from which a client computer downloads file(s) or other web content (Hypponen: [0013]).

16. As per claim 20, Hypponen discloses a network based anti-virus system according to claim 14. Hypponen further discloses the system comprising: wherein said anti-virus host computer does not specifically fight against viruses; wherein the purpose of said comparison is to find out if said inspected files and other web content are or are not non-wanted / unacceptable instead of if they are possibly virus infected (Hypponen: [0006]-[0010]; [0035]-[0038]).

17. As per claim 23, Hypponen discloses a network based anti-virus system according to claim 14. Hypponen further discloses the system comprising: wherein it is not done said identification comparison, and said identification(s) of said files) or other web content is not delivered to an anti-virus host computer (Hypponen: [0006]-[0010]); wherein an anti-virus host computer provides to a said intermediate computer a list of one or more of the following harmful or potentially harmful: (a) files or other web content, (b) publishers, (c) web sites, (d) host computers (Hypponen: [0006]-[0010]; [0035]-[0038]); wherein when a client computer

downloads file(s) or other web content from the network, said intermediate computer compares identification(s) of said file(s) or other web content to the items in said intermediate computer retained list, and if a said identification matches in certain extent any of said items, then: (a) it is performed safety measures, (b) and / or, said intermediate computer notifies said client computer and / or the user of said client computer about the results of said intermediate computer performed comparison (Hypponen: [0006]-[0010]; [0035]-[0038]).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 5, 6, 8, 11, 12, 16-19, 21, 22, and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen in view of Bates et al. U.S. Pat. No. 6721721 (hereinafter Bates).

20. As per claim 5, Hypponen discloses a network based anti-virus system according to claim 4. Hypponen further discloses the system comprising: wherein said stored identifications of files are stored identifications of known virus infected files (Hypponen: [0035]); wherein said stored identifications are in a database kept by said anti-virus host computer (Hypponen: [0035]); wherein said (a) and/or (b) type actions which are performed on the basis of the results of said comparison, are performed when a said delivered identification matches or resembles in certain

extent any of said stored identifications (Hypponen: [0035]; [0038]); wherein said safety measures are performed by requesting /causing said client computer and optionally also said anti-virus host computer to perform safety measures (Hypponen: [0038]). Hypponen does not explicitly disclose wherein said stored identifications of other web content are stored identifications of other known virus infected web content. However, Bates discloses a anti-virus database used to store virus status information including the types of file, name of the file, checksum, timestamp, etc. so that an URL can be checked prior to deliver the content to client device (Bates: column 13 lines 24-42). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to include more information to detect potential virus infected file that are not complicated including the name and types of virus files because types of file and names of the file are simple criteria to detect potential virus infected files. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates within the system of Hypponen because it improves the efficiency and resources of central anti-virus server to detect malicious files.

21. As per claim 6, Hypponen as modified discloses a network based anti-virus system according to claim 5. Hypponen further discloses the system comprising: wherein a said delivered identification consists of (a) file identification information, (b) and/or, data identification information (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein a said stored identification consists of (a) file identification information, (b) and/or, data identification information (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said file identification information comprises one or more of the following properties of the file or other web content to

which said file identification belongs: (a) source URL-address or other type of address, (b) source computer URL-address or other type of address, (c) name, (d) type, (e) content type, (f) size, (g) creation date, (h) version number, (i) publisher, (j) authentication certificate, (k) or, other properties (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said data identification information of the file or other web content to which said data identification belongs, comprises: (a) a check-sum or any identification value based upon the data of said file or other web content. (b) and / or, data sample picked according to a certain pattern, algorithm or other rule from said file or other web content, (c) or, all data of said file or other web content (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said file identification information and said data identification information is delivered to said anti-virus host computer either: (a) solely from said client computer, (b) solely from the respective source host computer(s) of said file(s) or other web content which file identification information anal data identification information it is question of, (c) or, partly from said client computer and partly from said respective source host computer(s) (Hypponen: [0006]-[0010]).

22. As per claim 8, Hypponen as modified discloses a network based anti-virus system according to claim 5. Hypponen as modified further discloses the system comprising: wherein said anti-virus host computer optionally informs / alarms said client computer and / or the user of said client computer only if the results of said comparison indicate a security threat or potential security threat, and optionally provides for said client computer and / or the user of said client computer a risk rating depicting the level of said security threat (Hypponen: [0038]); wherein said anti-virus host computer optionally informs said client computer and / or the user of said

client computer about the results of said comparison regardless of the type of said results, and optionally provides for said client computer and / or the user of said client computer a risk rating depicting the level of security threat indicated by said results (Hypponen: [0038]).

23. As per claim 11, Hypponen discloses a network based anti-virus system according to claim 10. Hypponen discloses the system comprising: wherein said stored identifications of files are stored identifications of known non-wanted/unacceptable files; wherein said stored identifications of other web content are stored identifications of other known non-wanted / unacceptable web content (Hypponen: [0035]: file type). In addition, Bates more explicitly discloses a anti-virus database used to store virus status information including the types of file, name of the file, checksum, timestamp, etc. so that an URL can be checked prior to deliver the content to client device (Bates: column 13 lines 24-42). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to include more information to detect potential virus infected file that are not complicated including the name and types of virus files because types of file and names of the file are simple criteria to detect potential virus infected files. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates within the system of Hypponen because it improves the efficiency and resources of central anti-virus server to detect malicious files.

24. As per claim 12, Hypponen as modified discloses a network based anti-virus system according to claim 5. Hypponen as modified further discloses the system comprising: wherein

said other web content comprises one or more of the following: (a) web pages, (b) independent program scripts or other client computer processed components, (c) e-mail messages, (d) e-mail message attachments, (e) or, any data which a client computer can download from the network (Hypponen: [0013]).

25. As per claim 16, Hypponen discloses a network based anti-virus system according to claim 14. Hypponen further discloses the system comprising: wherein said stored identifications of files are stored identifications of known virus infected files (Hypponen: [0035]); wherein said stored identifications of other web content are stored identifications of other known virus infected web content (Hypponen: [0035]); wherein said stored identifications are in a database kept by said anti-virus host computer; wherein said (a) and / or (b) type actions which are performed on the basis of the results of said comparison, are performed when a said delivered identification matches or resembles in certain extent any of said stored identifications; wherein said safety measures are performed by requesting / causing one or more of the following computers to perform safety measures: (a) a said intermediate computer, (b) said client computer, (c) said anti-virus host computer (Hypponen: [0038]). Bates further discloses a anti-virus database used to store virus status information including the types of file, name of the file, checksum, timestamp, etc. so that an URL can be checked prior to deliver the content to client device (Bates: column 13 lines 24-42). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to include more information to detect potential virus infected file that are not complicated including the name and types of virus files because types of file and names of the file are simple criteria to detect potential virus infected files. Therefore, it

would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates within the system of Hypponen because it improves the efficiency and resources of central anti-virus server to detect malicious files.

26. As per claim 17, Hypponen as modified discloses a network based anti-virus system according to claim 16. Hypponen as modified further discloses the system comprising: wherein a said delivered identification consists of (a) file identification information, (b) and / or, data identification information (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein a said stored identification consists of (a) file identification information, (b) and / or, data identification information (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said file identification information comprises one or more of the following properties of the file or other web content to which said file identification belongs: (a) source URL-address or other type of address, (b) source computer URL-address or other type of address, (c) name, (d) type, (e) content type, (f) size, (g) creation date, (h) version number, (i) publisher, (j) authentication certificate, (k) or, other properties (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said data identification information of the file or other web content to which said data identification belongs, comprises: (a) a check-sum or any identification value based upon the data of said file or other web content, (b) and / or, data sample picked according to a certain pattern, algorithm or other rule from said file or other web content, (c) or, all data of said file or other web content (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said file identification information and said data identification information is delivered to said anti-virus host computer either: (a) solely from a said intermediate computer, (b) solely from the respective source host computer(s)

of said file(s) or other web content which file identification information and data identification information it is question of, (c) or, partly from a said intermediate computer and partly from said respective source host computer(s) (Hypponen: [0006]-[0010]).

27. As per claim 18, Hypponen as modified discloses a network based anti-virus system according to claim 16. Hypponen as modified further discloses the system comprising: wherein said requesting / causing to perform said safety measures is done by said anti-virus host computer (Hypponen: [0038]); wherein said informing about the results of said comparison is done by a said intermediate computer; wherein said safety measures comprise one or more of the following: (a) a said intermediate computer performs a virus scan for said file(s) or other web content which said anti-virus host computer has determined to be a security threat in certain extent (Hypponen: [0006]-[0010]; [0035]-[0038]). (b) a said intermediate computer sends said security threat file(s) or other web content to be virus scanned by said anti-virus host computer (Hypponen: [0006]-[0010]; [0035]-[0038]). (c) a said intermediate computer prevents the download of said security threat file(s) or other web content through said intermediate computer (Hypponen: [0006]-[0010]; [0035]-[0038]); wherein optionally said anti-virus host computer alternatively acquires independently said security threat file(s) or other web content, and performs a virus scan for said security threat file(s) or other web content (Hypponen: [0006]-[0010]; [0035]-[0038]).

28. As per claim 19, Hypponen as modified discloses a network based anti-virus system according to claim 18. Hypponen as modified further discloses the system comprising: wherein a

said intermediate computer optionally informs / alarms said client computer and / or the user of said client computer only if the results of said comparison indicate a security threat or potential security threat, and optionally provides for said client computer and / or the user of said client computer a risk rating given by said anti-virus host computer, said risk rating depicting the level of said security threat (Hypponen: [0038]); wherein a said intermediate computer optionally informs said client computer and / or the user of said client computer about the results of said comparison regardless of the type of said results, and optionally provides for said client computer and / or the: user of said client computer a risk rating given by said anti-virus host computer, said risk rating depicting the level of security threat indicated by said results (Hypponen: [0038]).

29. As per claim 21, Hypponen discloses a network based anti-virus system according to claim 20. Hypponen further discloses the system comprising: wherein said stored identifications of files are stored identifications of known non-wanted I unacceptable files; wherein said stored identifications of other web content are stored identifications of other known non-wanted / unacceptable web content (Hypponen: [0035]: file type). In addition, Bates more explicitly discloses a anti-virus database used to store virus status information including the types of file, name of the file, checksum, timestamp, etc. so that an URL can be checked prior to deliver the content to client device (Bates: column 13 lines 24-42). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to include more information to detect potential virus infected file that are not complicated including the name and types of virus files because types of file and names of the file are simple criteria to detect potential virus

infected files. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates within the system of Hypponen because it improves the efficiency and resources of central anti-virus server to detect malicious files.

30. As per claim 22, Hypponen as modified discloses a network based anti-virus system according to claim 16. Hypponen as modified further discloses the system comprising: wherein said other web content comprises one or more of the following: (a) web pages, (b) independent program scripts or other client computer processed components, (c) e-mail messages, (d) e-mail message attachments, (e) or, any data which a client computer can download from the network (Hypponen: [0013]: different transit node for different data).

31. As per claim 24, Hypponen discloses a network based anti-virus system especially for wide area networks, like the Internet, comprising: a client computer, which is any computer in the network; an intermediate computer which is able to prevent downloading of files and / or other web content from the network to said client computer (Hypponen: [0006]-[0010]; [0035]-[0038]); wherein when said client computer downloads a file or other web content from the network, and if the identification of said file or other web content matches or resembles in certain extent any of the identifications in a database of the identifications of known virus infected files or other virus infected web content, then said intermediate computer: (a) prevents said download of said file or other web content, (b) or, requests / causes said client computer to destroy said file or other web content from said client computer if said client computer has

already downloaded said file or other web content, (c) and / or, optionally informs said client computer or the user of said client computer about said security threat (Hypponen: [0006]-[0010]; [0035]-[0038]); wherein said identifications in said database are not signatures of virus code, but rather represent the identities of the virus infected files or other virus infected web content self wherein a said identification in said database either: (a) belongs to a specific file or other web content, (b) does not belong to any specific file or other web content, but is rather an identification filter, (c) or, partly belongs to a specific file or other web content, and partly is a said identification filter (Hypponen: [0006]-[0010]; [0035]-[0038]). Furthermore, Bates discloses a anti-virus database used to store virus status information including the types of file, name of the file, checksum, timestamp, etc. so that an URL can be checked prior to deliver the content to client device (Bates: column 13 lines 24-42). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to include more information to detect potential virus infected file that are not complicated including the name and types of virus files because types of file and names of the file are simple criteria to detect potential virus infected files. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates within the system of Hypponen because it improves the efficiency and resources of central anti-virus server to detect malicious files.

32. As per claim 25, Hypponen as modified discloses a network based anti-virus system according to claim 24. Hypponen as modified further discloses the system comprising: wherein said intermediate computer is: (a) a server of the local area network, (b) a server of the internet

service provider, (c) a network node computer, (d) or, a source host computer from which said client computer downloads file(s) or other web content (Hypponen: [0013]).

33. As per claim 26, Hypponen as modified discloses a network based anti-virus system according to claim 24. Hypponen as modified further discloses the system comprising: wherein a said identification in said database consists of (a) file identification information, (b) and / or, data identification information (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said identification of said inspected file or other web content consists of: (a) file identification information, (b) and / or, data identification information (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said file identification information comprises one or more of the following properties of the file or other web content to which said file identification belongs: (a) source URL-address or other type of address, (b) source computer URL-address or other type of address, (c) name, (d) type, (e) content type, (f) size, (g) creation date, (h) version number, (i) publisher, (j) authentication certificate, (k) or, other properties (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said data identification information of the file or other web content to which said data identification belongs, comprises: (a) a check-sum or any identification value based upon the data of said file or other web content (Hypponen: [0035]; Bates: column 13 lines 24-42), (b) and / or, data sample picked according to a certain pattern, algorithm or other rule from said file or other web content, (c) or, all data of said file or other web content (Hypponen: [0035]; Bates: column 13 lines 24-42).

34. Claims 7, 9, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen in view of Bates and further in view of Bates et al. U.S. Pat. No. 6785732 (hereinafter Bates2).

35. As per claim 7, Hypponen as modified discloses a network based anti-virus system according to claim 5. Hypponen as modified further discloses the system comprising: wherein said requesting / causing to perform said safety measures is done by said anti-virus host computer (Hypponen: [0038]); wherein said informing about the results of said comparison is done by said anti-virus host computer (Hypponen: [0038]) and the anti-virus host computer will scan the file for virus (Hypponen: [0036]-[0038]). Hypponen as modified does not explicitly disclose wherein said safety measures comprise one or more of the following: (a) said client computer performs a virus scan for said file(s) or other web content which said anti-virus host computer has determined to be a security threat in certain extent. (b) said client computer sends said security threat file(s) or other web content to be virus scanned by said anti-virus host computer, (c) said client computer destroys said security threat file(s) or other web content, (d) said client computer performs a virus scan in said client computer, the software for said virus scan optionally being provided by said anti-virus host computer; wherein optionally said anti-virus host computer alternatively acquires independently said security threat file(s) or other web content, and performs a virus scan for said security threat files) or other web content. However, Bates2 discloses the anti-virus server or the client can check the virus and if new virus is found, new virus information can be transmitted to database to inform other computers of the new virus (Bates2: column 2 lines 10-46). It would have been obvious to one having ordinary

skill in the art at the time of applicant's invention to notify the client so that the client can check/scan the file for virus upon notification by the server because the virus checker can be centralized or decentralized. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates2 within the combination of Hypponen-Bates because it reduces the burden of the server to check files of all clients.

36. As per claim 9, Hypponen as modified discloses a network based anti-virus system according to claim 5. Hypponen as modified further discloses the system comprising: wherein said anti-virus host computer keeps database of the identifications of the files and / or other web content which the client computers or the users of client computers have downloaded from the network, each said identification being stored in said database in connection of the respective downloading of said file or other web content to which said identification belongs (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said anti-virus host computer retains information about one or more of the following: (a) old and / or newly detected virus infections, (b) old and / or newly detected security threats, (c) old and / or newly determined security risk ratings, (d) personal download statistics, for the files and / or other web content which a client computer or the user of said client computer has earlier downloaded from the network (Hypponen: [0035]; Bates: column 13 lines 24-42); wherein said anti-virus host computer informs / alerts the respective client computer and / or the user of said respective client computer, when said anti-virus host computer retained information on the part of any of (a) through (c) changes in certain way (Hypponen: [0038]). Hypponen as modified does not explicitly disclose said client

computer and / or the user of said client computer being optionally able to access said anti-virus host computer retained information; wherein if said anti-virus host computer announces said anti-virus host computer retained information on the part of any of (a) through (c) to have changed alarming enough for certain files(s) or other web content, then the respective client computer optionally: (a) destroys said file(s) or other web content from said client computer, (b) and / or, performs a virus scan in said client computer, the software for said virus scan optionally provided by said anti-virus host computer. However, Bates2 discloses the server may download virus checker to client and the client may perform the security measures and database is provided to store information about newly found virus including file location, names, etc. (Bates: column 2 lines 34-56). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to notify the client so that the client can check/scan the file for virus upon notification by the server because the virus checker can be centralized or decentralized. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates2 within the combination of Hypponen-Bates because it reduces the burden of the server to check files of all clients.

37. As per claim 27, claim 27 encompasses the same scope as claim 9. Therefore, claim 27 is rejected based on the same reason set forth in claim 9.

38. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen in view of Bates2.

39. As per claim 13, Hypponen discloses a network based anti-virus system according to claim 1. Hypponen does not explicitly disclose the system comprising: wherein it is not done said identification comparison, and said identification(s) of said files) or other web content is not delivered to an anti-virus host computer; wherein an anti-virus host computer provides to a client computer a list of one or more of the following harmful or potentially harmful: (a) files or other web content, (b) publishers, (c) web sites, (d) host computers; wherein when said client computer downloads file(s) or other web content from the network, said client computer compares identification(s) of said file(s) or other web content to the items in said client computer retained list, and if a said identification matches in certain extent any of said items, then: (a) it is performed safety measures, (b) and / or, said client computer notifies the user of said client computer about the results of said client computer performed comparison. However, Bates2 discloses the virus checker is downloaded to the client computer and the client computer perform necessary security measures (Bates2: column 2 lines 10-56). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to notify the client so that the client can check/scan the file for virus upon notification by the server because the virus checker can be centralized or decentralized. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Bates2 within the combination of Hypponen-Bates because it reduces the burden of the server to check files of all clients.

Conclusion

40. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ji et al. U.S. Pat. No. 5623600 discloses virus detection and removal apparatus for computer networks.

Chen et al. U.S. Pat. No. 5832208 discloses anti-virus agent for use with databases and mail servers.

Tso et al. U.S. Pat. No. 6088803 discloses system for virus-checking network data during download to a client device.

Wells U.S. Pat. No. 6338141 discloses method and apparatus for computer virus detection, analysis, and removal in real time.

Le Pennec et al. U.S. Pub. No. 20010020272 discloses method and system for caching virus-free file certificates.

Tarbotton et al. U.S. Pat. No. 6757830 discloses detecting unwanted properties in received email messages.

Glover U.S. Pat. No. 6763466 discloses fast virus scanning.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100